New ways for policy-makers to interact with citizens through open social network sites - a report on initial results

Matthew Addis, Steve Taylor, Bassem I. Nasser
IT Innovation Centre, University of Southampton, UK.

Somya Joshi, Evika Karamagioli
Gov2u, Greece.

Timo Wandhoefer
Leibniz Institute for the Social Sciences, Germany

Freddy Fallon
Hansard Society, UK.

Rachel Fletcher, Caroline Wilson,
Institute for Law and the Web at Southampton, University of Southampton, UK.

For more information contact Matthew Addis (mja@it-innovation.soton.ac.uk) or use the contact points on the WeGov website (www.wegov-project.eu)

ABSTRACT

Social networking sites (SNS) provide major new opportunities for policy-makers (eGovernment) to engage with citizens (eSociety). The European Commission supported WeGov project is developing a software toolkit that allows policy-makers to take full advantage of a wide range of existing and well established social networking sites (Facebook, Twitter, Bebo, WordPress etc.) to engage citizens in two-way dialogs as part of governance and policymaking processes. The tools will make it possible to detect, track and mine opinions and discussions on policy oriented topics and allow discussions to be seeded and stimulated through injection of policy discussion points into relevant communities in a secure and managed way. A key feature of our approach is to allow policy-makers to move away from the limitations inherent in the current practice of using bespoke and dedicated platforms (e.g. specific opinion soliciting websites hosted by government departments) and instead make full use of the high levels of participation and rich discussions that already take place in existing social networking sites. In this paper we present early results of the project. This includes: a set of scenarios for using SNS as part of the policy making process; the legal and ethical issues this entails (e.g. privacy, data protection, defamation); the use of an information security risk assessment methodology to identify potential further issues and their countermeasures; and an overview of the new software technologies needed to make this new mode of interaction between citizen and policy-maker quick, simple, reliable and cost effective.

INTRODUCTION

WeGov is a recently started three year project supported by the European Commission under the FP7 ICT programme. WeGov will develop new tools that allow policy-makers to interact with and understand the opinions of citizens by using well established public social networking sites (facebook, twitter, wordpress etc.). The explosion in use of SNS throughout society provides unprecedented opportunities for policy-makers (eGovernment) to engage with citizens (eSociety) through existing, open, well used and familiar settings. This is in stark contrast to the more common approach of using dedicated, bespoke, constrained and very

often underused web-based opinion soliciting platforms. In a sense, these existing sites are very much like 'walled gardens'; they are carefully constructed and can look very inviting, but they have rigid boundaries, limited admission, restrictive rules of use, and more often than not they are empty of visitors! In contrast, WeGov aims to use existing and popular public SNS that function much more like municipal parks – large, unconstrained spaces where many people come together for a diverse set of reasons where discussion is far more open, wide reaching and representative of the community.

Some of the approaches already tried for eParticipation are reviewed in the Hansard Society's digital dialogs report (third phase) [2]. In particular, the case study of No10 Downing Street is an exemplar on the problems that WeGov sets out to address. This case study reviews what happened when a discussion website (DebateMapper) was set-up to support Tony Blair's series of lectures when he left office. There were 309 invitees to the site (e.g. journalists), with 240 invited via Reuters and 69 invited by the Hansard Society. 7% of the invitees registered, including 25% of the Hansard Society invitees and 2% of the Reuters invitees. Only 2 of Hansard Society invitees contributed to the map – via edits and comments. None of the media invitees contributed directly to the map. So, in short, almost nobody added information to the bespoke DebateMapper website. This was primarily because many of those invited to participate were from the media and already had alternative and favoured ways of airing their views, e.g. in newspaper columns. The comments and blogs attached or linked to these other established channels was where the discussion really took place. This is a prime example of discussion taking place where it is most natural and using the tools that are most familiar to those involved – with an attempt to move the location and structure of the discussion, i.e. to DebateMapper, resulting in little impact. Public use of social network sites for political discussion be it about local, national or international issues, is exactly the same.

For WeGov as an ICT project, the main focus is research and development of new software technologies to support two-way 'in-situ' dialogs between policy-makers and citizens in one or more open social network sites. In making this shift, there is a clear need to consider a range of legal, ethical and technical issues, as well as to have clear motivating scenarios that can be used to drive the project forward and test the results of the project as they are created. It is this mix of issues and how they can be reconciled that forms the substance of this paper.

MOTIVATING SCENARIOS

At the time of writing, WeGov is at the end of the first 6 months of its 30 month duration and in this time has focussed on initial definition of a set of live field trials for the later stages of the project. Scenarios for these field trials have been developed by the Hansard Society in the UK, The Leibniz Institute for the Social Sciences (GESIS) in Germany, and Government to You (Gov2u) in Greece. The scenarios have been developed in tandem with a review by The Institute for Law and the Web in Southampton to ensure legal and ethical issues are properly addressed. At the same time, the planned trials provide direction for the main technology R&D work to be done in the project and have been analysed from this perspective to ensure they are technically feasible. The scenarios are expected to evolve as the project progresses and are to some extent in their formative stage, therefore this paper presents an overview rather than specific details.

CONSUMER PROTECTION SCENARIO

Gov2u plans to use the WeGov toolkit for regional e-participation in consumer protection policy by building upon scenarios developed during the VoicE [1] project. The objective is more informed decision making within European

regions, with specific reference to regional policy-makers in the European Parliament. VoicE was designed as a trial project, implementing a new regional model of e- participation in the European Union (EU) which places a high emphasis on platform marketing, editorial preparation and integration into the surrounding political institutions. In this regard, VoicE provided a platform that served as an interface between decision-makers in the European Parliament, the European Commission (EC), the Committee of Regions and citizens while using and testing new forms and methods of civic participation in the day-to-day legislative work in the EU. In terms of content, the project focused on the policy field of consumer protection.

The scenario in WeGov focuses on the policy field of consumer protection in the EU. Citizens engaging in debates on SNS, will be able to share their opinions with political decision-makers on issues, which are in the legislative pipeline at that very moment, just before relevant decisions are to be made. By being allowed to participate and be informed about the process, as well as where their input fits in, the citizens have a greater potential to learn about the legislative process. This way, they will be able to meaningfully express their opinions on the legislation in the field of consumer protection by delivering real inputs during the proposal formation stage or the debate on draft legislation in this field.

The WeGov toolkit will be used by the policy-makers to enable them to gather the most topical, relevant and popular information concerning consumer protection issues for their region. Functionalities such as hot topic extraction, tag clouds, opinion mining etc, will be employed via the WeGov toolkit in order to enable MPs and decision makers to monitor and evaluate in an organized manner, the flow of citizen inputs scattered across diverse SN sites.

To ensure easy use by the policy-maker, they will need to be presented with a dashboard wherein all the diverse inputs from citizens are collated, aggregated, analysed and presented using visualization technologies that make the data more accessible and easy to understand. At another level, the policy-maker needs to post comments, opinions and calls back on the SNS based on the analysis and data received on the relevant legislative issues concerning consumer protection. Thus the Gov2u scenario requires the integration of various functionalities within the WeGov toolkit, allowing policy-makers to tap into debates taking place in SNS.

The process begins with identifying a relevant topic being discussed on a SNS, where citizens are already freely commenting and debating the issue at hand. The policy-maker can become part of this discussion should they wish. This mode of interaction shown in Figure 1, which targets discussions on existing groups on Facebook following the Policy-maker's criteria. The scenario starts at the top with citizens who are already discussing consumer protection issues.

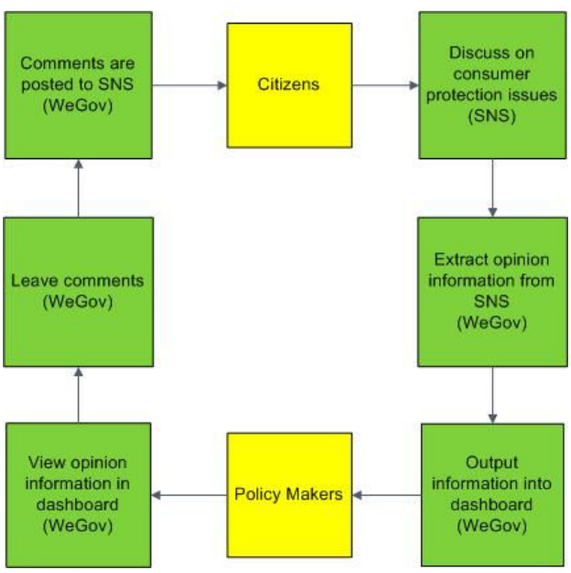

Figure 1 consumer protection scenario: discovering and contributing to existing debates

If debates are not already taking place, or if the policy-maker wants to explicitly stimulate a specific discussion, then there is the need for a process whereby the policy-maker can be proactive and launch a discussion, as shown in Figure 2 which starts at the top this time with the policy-maker. These debates will take place on either the policy-maker's page on a SNS or on identified discussion group pages, which are searched and selected by policy-makers. The citizens then log into these debates (this also acts as a point where we seek consent), and add their voice/ opinions.

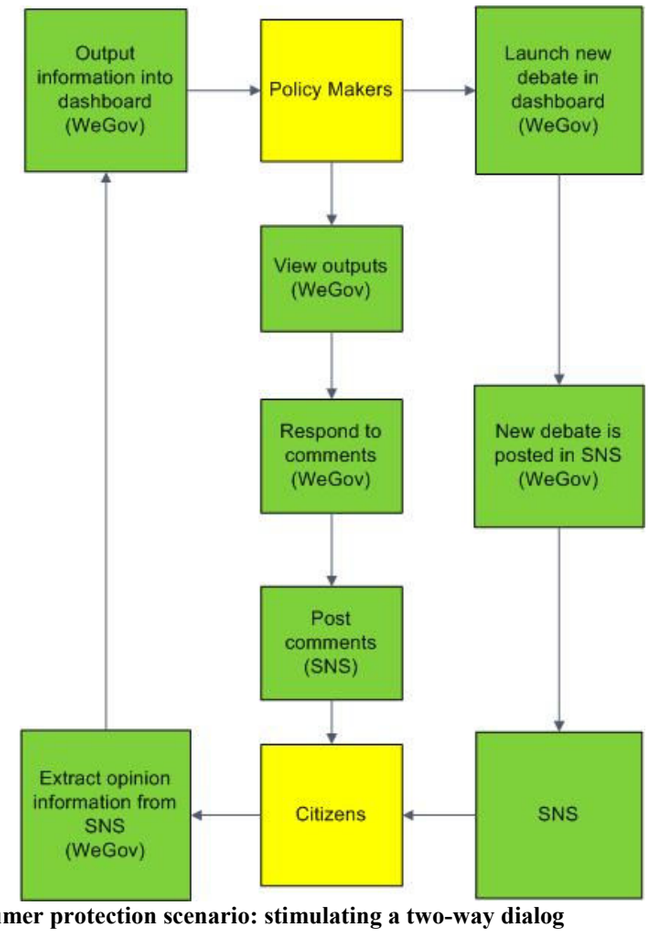

Figure 2 consumer protection scenario: stimulating a two-way dialog

The consumer protection scenario has been developed by involving the Regional Government of Valencia in Spain and the other involving Regional Authorities in Germany. The WeGov toolkit will be assessed against the following benefits anticipated by Baden-Württemberg: (a) more direct participation of the citizen via SNS in the political debate, (b) direct citizens ideas and opinions provided to the Members of Regional Government and German Representation in the EU Parliament to work with; (c) increased public awareness of the legislative process, and (d) valuable feedback to the public forums from the policy-makers directly. In the Valencia case, the following benefits are anticipated by the Regional Government: (a) flow of ideas and opinions for the policy-makers/ representatives to work with; (b) increased public awareness of the legislative process; and (c) experience on the use of semantic technology and argument visualization technology.

DISPOSAL OF NUCLEAR WASTE SCENARIO

The second WeGov scenario organised by GESIS focuses on the long-term storage of nuclear waste in Germany at the Gorleben facility [3] and the long-standing debate that surrounds the validity of this choice [4]. The objectives is for

the WeGov toolkit to support the briefing of members of the German Parliament when taking part in decision-making of German politics by ensuring that they are fully aware of the extent and views of citizens surrounding hot topics in politics and society such as Gorleben. This includes briefing politicians about the statements of other politicians and what are their decisions concerning hot topics. Normally this information is prepared by the personal 'Abstractor'. Therefore, the GESIS scenario is one of supporting the Abstractor to build up an online community to discuss hot topics and obtain structured opinions of citizens as well as by engaging experts and using third party online surveys. As with the consumer protection scenario from Gov2u, there are distinct modes of interaction between the stakeholder (Abstractor in this case) and the citizen.

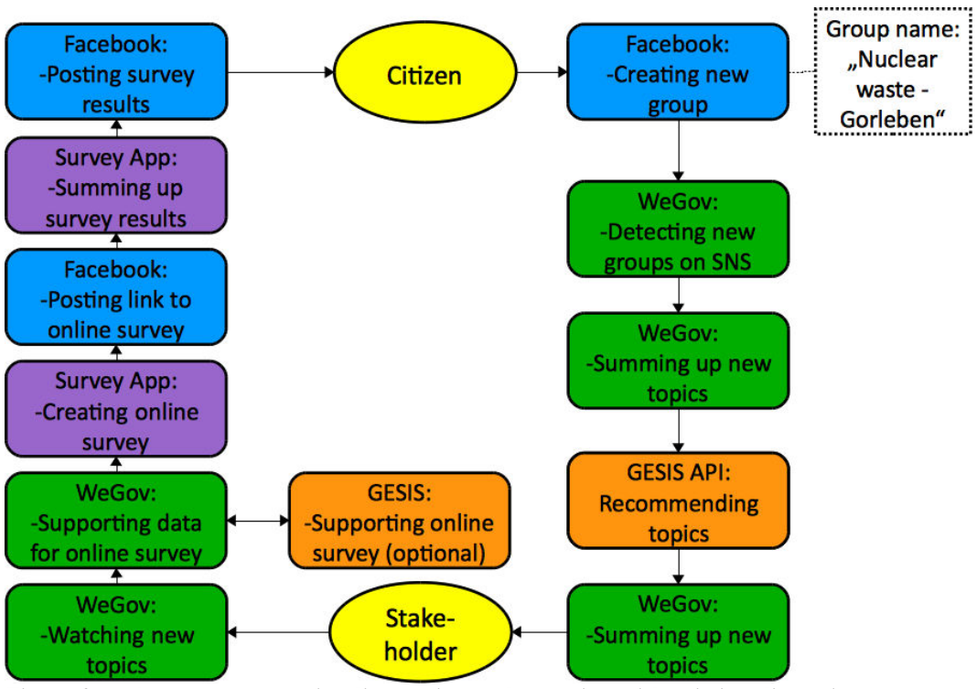

Figure 3 nuclear waste scenario: discovering and engaging with existing discussions

In the first mode of interaction the WeGov toolkit allows the stakeholder to seek out existing and relevant discussions and then support the stakeholder to interact with the citizens in the selected discussions. This is shown in Figure 3 showing an example where a Facebook group started by a citizen is located and then used as the basis of a survey by the stakeholder. In the end the eCitizens also benefit, because their opinions are heard and the online survey results are posted back on SNS. The starting point is where a citizen creates a new group "Nuclear waste – Gorleben" to discuss the set of problems. GESIS has a direct role in the scenario through services they supply for defining and executing surveys and also through their "Search Term Recommender – STR" [5] which helps the stakeholder in using the most appropriate terms when searching SNS for existing discussions.

In the second mode of interaction the stakeholder is more proactive and wishes to stimulate a discussion. In the example shown in Figure 4, this scenario starts with the stakeholder posting a new YouTube video, e.g. to start a new debate or present a particular point of view. The first stage of the process involves citizens commenting on the video using YouTube. The stakeholder in response then creates a survey to capture more structured comments and uses a facebook group to provide the gateway to the survey and feedback of the results to the community.

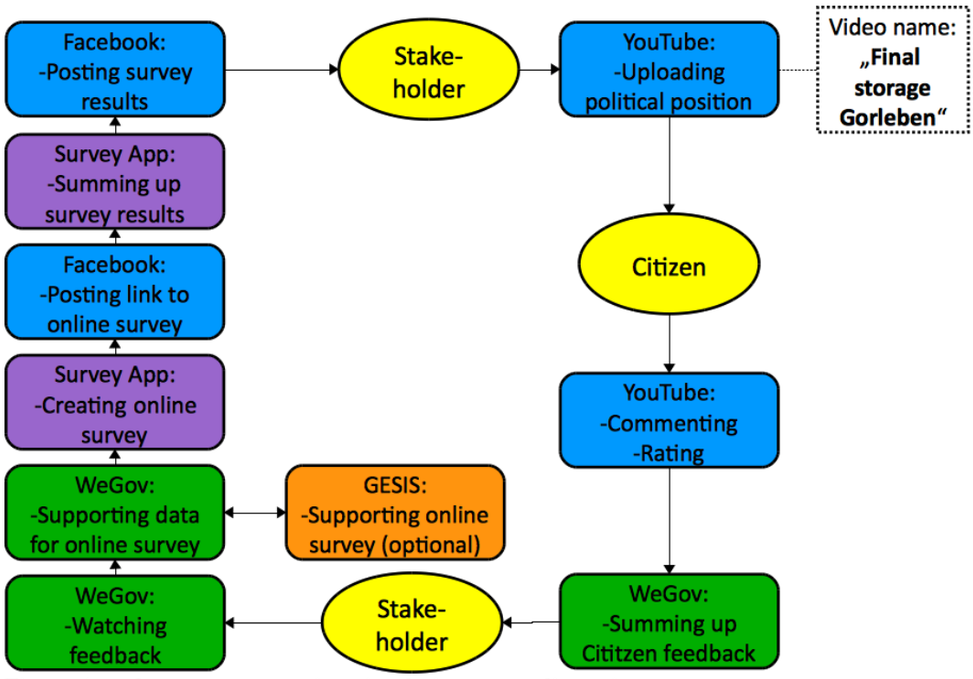

Figure 4 nuclear waste scenario: stimulating a new discussion

PUBLIC HEALTHCARE SCENARIO

The third WeGov scenario being driven by the Hansard Society focuses on opinion on public healthcare in the UK. Here an existing health service comment website already exists and was set up originally in 2006 in the northwest of England. It is independent of the National Health Service (NHS) and government, and aims to give patients a user-generated resource providing information about the quality of health services around the UK. Unlike some other current initiatives in Britain, it gives everyone the ability to view, use, and add to it.

The site has attracted a high level of mainstream media interest, helping with its publicity. It has also been rated highly by those who use it, and attracts repeat visits from around 40%. Users tend to be demographically mixed, with more female visitors and all age-ranges are represented. The majority (just under 70%) of visitors find responses posted by health service providers useful; however users are not always clear as to whether health service providers are considering their opinions.

Whilst an increasing number of hospitals and Primary Care Trusts are subscribing to the site, these are not displayed on the site, so patients do not necessarily know whether their local services are listening. A large proportion of visitors are committed to using this health services comment site, with around 30% of users saying that they are more likely to get more involved with health policy and activism as a result of their experiences using the site. A large proportion of those providing feedback about the site work for the NHS: from their perspective, the site offers useful information about what works and where there is room for improvement in patient care. From the perspective of the public, meanwhile, the site provides a useful way of framing decisions about health care.

However, whilst the site is rated highly by its users, there is still considerable scope for opening up the debate to a wider audience using WeGov's tools to allow health service comment to occur through both Twitter and Facebook.

Again there are two main modes of interaction between the stakeholder (decision maker in this case, e.g. policy-maker in a local healthcare trust) and the citizens. In the first mode, health service staff want to be able to explore existing

citizens' opinions about the quality of their services, by monitoring relevant debates on SNS, and responding publicly. This is shown in Figure 5.

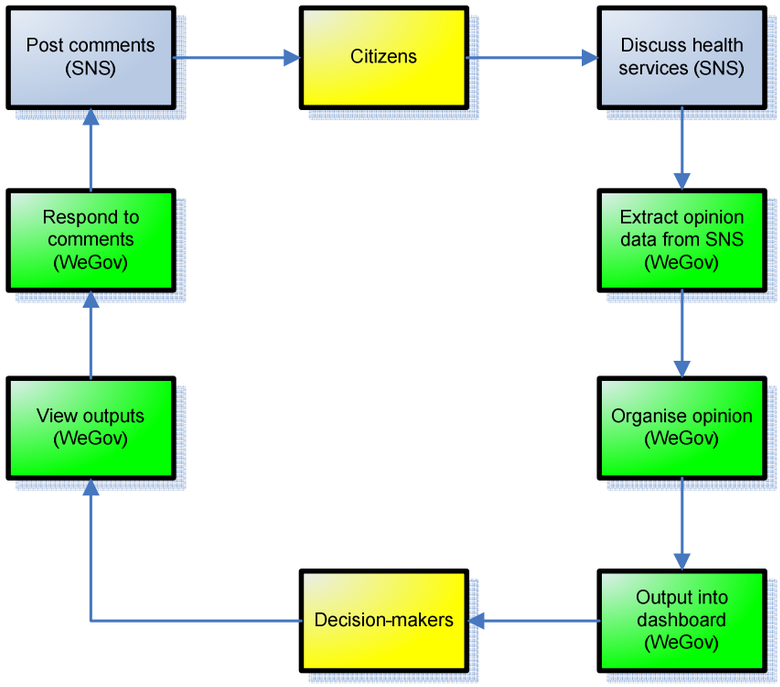

Figure 5 public healthcare scenario: monitoring and participating in existing discussions

In the second mode, health service providers who are interested in citizens' opinions on specific issues want to launch new topics, collect responses and produce public responses. Figure 6 shows the different processes involved in this scenario, starting with a decision-maker launching a question or topic of discussion that they want input from citizens on, which is then posted to the social networks.

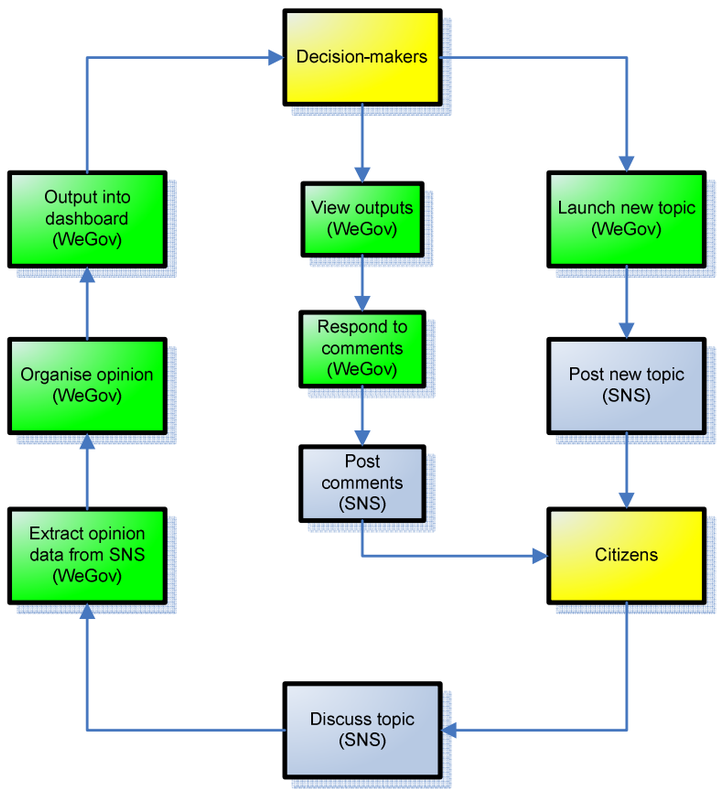

Figure 6 public healthcare scenario: creating new discussions

The WeGov toolkit then extracts opinion data from the social networking sites, along with the citizen's username, age, gender, and location and organises this data based on the citizen's age, gender, and location, along with the popularity ranking of comments (by number of followers, retweets, 'likes' on Facebook etc.). Decision-makers are then capable of responding to the comments that have been collected and these responses are then posted back onto the social networks. Citizens are then able to view the responses to their comments on the social networks that they use and comment further on the topic.

SUMMARY OF SCENARIOS

Each of the three scenarios for the project has several modes of interaction between the main stakeholder (e.g. policy-maker) and the citizens that they seek to understand or engage with. These modes centre on who first instigates the discussion and hence whether the stakeholder is initially a proactive or passive participant. In all cases the stakeholder ends up engaging with the citizens and in all cases the interaction is cyclic, i.e. a dialog takes place that evolves over time.

The common threads of monitoring existing discussions, seeding new ones, and the flow of feedback from policy-makers to users & vice versa is crucial to WeGov. We see in the Hansard case the scenario of the health service comment where the processes at work involve monitoring existing debates as well as seeding new ones. In the Gov2u case these processes are further reinforced within the context of consumer protection. We find here a two way flow between policy-makers keeping a hand on the pulse of public opinion and debate, as well as feeding back their comments and insights to citizens who pose questions and raise issues. Finally in the GESIS case on long-term nuclear waste storage, we find within the context of policy and political science a similar exchange between academics, members of parliament and the wider stakeholder base.

TOOLKIT APPROACH

The need to support the various modes of interaction in the project scenarios, in particular the iterative nature of the dialog, is a main driver for the technological development work being done by the project. For example, locating existing discussions within large SNS sites is potentially like finding needles in a haystack and requires sophisticated topic-opinion detection and analysis tools as well as making full use of SNS and search engine APIs to find possible matching pages, groups, individuals, tags, comments etc. Presenting complex information in an easy to understand and transparent way is essential if the toolkit is to be used in practice, including making it very easy for policy-makers to interact with multiple SNS in a consistent way and potentially at the same time.

The approach to the toolkit to be developed in WeGov is shown in Figure 7 which represents how the tools are used in a cycle of interaction between policy-maker and citizens. Working round this cycle counter clockwise starts with extraction tools that are used for retrieving information from a wide range of social network sites in a way that adheres to privacy and safeguarding measures. In particular, a common API is being developed across the SNS of interest. Information extracted from a SNS, e.g. comments in a Facebook group, are then processed using analytics tools so discussions in online communities can be understood in terms of the topics and opinions of participants. The result is topic-discussion-opinion data structures (e.g. graphs) that represent the topics dealt with and the opinions being expressed by people and how they relate to a debate, e.g. how they substantiate or counter a position, what arguments are used, the direction of a discussion, and its range of opinions or its weighing of different points of view. These data structures are then visualised and presented to the policy-maker through a dashboard which also provides access to tools for

communication and injection to allow the policy-maker to stimulate debates or respond to citizen concerns. Here the emphasis is how to define and automate the process of communication between policy-makers and citizens in a structured and rigorous way (important for transparency, provenance, ensuring conformance to policies, and also publication and reuse) and how to best place content (injection) into social network sites in order to stimulate a discussion (what, where and when).

Recognising that success of WeGov is far more than just technology, the policy-maker is supported by methodology, guidelines and best practice for use of WeGov techniques and tools when interacting with citizens on open social networking sites (shown on the right of the diagram). Full details of the WeGov technical approach, architecture and tools will be the subject of future publications.

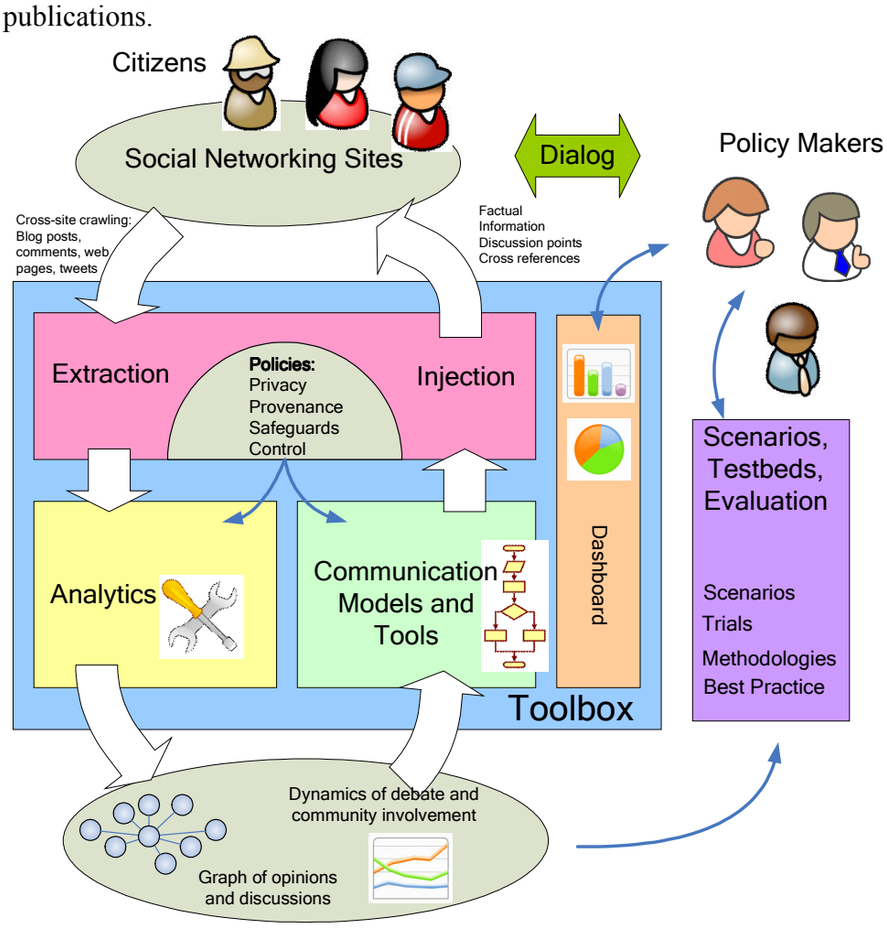

Figure 7 WeGov toolkit

LEGAL AND ETHICAL ANALYSIS

The use of third-party SNS by policy-makers to find hot political topics, gauge opinion, and engage citizens in debate brings with it a set of legal and ethical challenges. Many of these issues concern data protection for the users of SNS, but other areas that are important to consider are copyright, defamation, and direct marketing. The legal and ethical review presented here is necessarily restricted to a broad overview of EU law and legislation with a consideration of the law of England and Wales. This approach allows the scoping of both breadth (EU) and depth (one particular jurisdiction) of issues. It is important to note that EC law does not address all the areas relevant to the WeGov project, and where this is the case, different EC Member States are free to develop purely national legal solutions to such issues. However, divergence in legal approach is not limited to such areas: even where the EC has legislated on a particular legal topic, there may

still be significant differences in how each EC Member State addresses the same topic.

The rest of this section reviews these issues, in particular privacy, and then discusses the implications for the motivating scenarios of the project. Privacy is an internationally recognised fundamental human right, but lawyers and philosophers alike struggle to define it. We adopt Banisar's [6] four aspect approach, but focus on only two of the four elements i.e. 'informational privacy' and 'privacy of communications'; these being particularly pertinent to the WeGov project. The following sections highlight relevant EC Directives aimed at protecting these distinct but interrelated concepts.

DATA PROTECTION AND RETENTION

The principal EC Directive regulating the processing of personal data is Directive 95/46/EC (the 'Data Protection Directive') [7]. This was implemented in England and Wales by the Data Protection Act 1998. For Policy-makers the following questions must be considered:

Who is a data controller and who is a data processor?

- This distinction is important as processors are not obliged to comply with data protection legislation and reference should be made to the recent opinion of the Article 29 Working Party [8].
- Key to this issue is establishing who determines the purpose and means of the processing.
- Given the wide definition of 'processing' more than one entity might be making this determination, but the definition of 'data controller' provides for the possibility of pluralistic control.

How is processing defined?

- Processing is defined extremely widely by the Data Protection Directive and the processes undertaken in the WeGov scenarios would be caught by the definition.

Will the data being processed through the Toolkit be personal data?

- Does the data have a *'content'* element (about an individual), a '*purpose'* element (where the data might be used with the purpose to evaluate or treat an individual in a certain way) or a *'result'* element (where the data may impact upon an individual)?
- If so, is an individual identified or identifiable by that data? Identifiable is widely defined. It is considered that unless the data can be anonymised at the point of collection (i.e. from the SNS) that individuals are likely to remain identifiable in legal terms. Furthermore given the requirements of Policy-makers it is likely that they would wish to identify individuals for the purpose of data provenance and/or in order to engage with them.

What is sensitive data?

- Sensitive data is a special category of personal data. Where sensitive data is being processed, national and European legislation places additional obligations on data controllers.
- Sensitive data includes data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or where data processed concerns information about an individual's health or sex life.

What are the obligations placed on data controllers?

- The obligations contained with the Directive are transposed into national legislation, for example the Data Protection Act for England and Wales where these obligations form the eight data protection principles
    - First Principal – Fair and Lawful Processing & Conditions for Processing
    - Second Principal – Personal data to be used only for a specific purpose or purposes.
    - Third Principal – Personal data shall be adequate, relevant and not excessive
    - Fourth Principal – Keeping personal data up to date.
    - Fifth Principal – Adequate and necessary retention periods
    - Sixth Principal – Processing in accordance with data subjects' rights.
    - Seventh Principal – Implementation of adequate security and organisational measures.
    - Eight Principal – Transfers outside of the EEA.

Notification

- Data controllers, unless exempt, must provide notification to their national data protection authority

How best to ensure compliance?

- Both the EU Article 29 Working Party and the UK's national data protection authority, the Information Commissioner's Office (ICO) have produced numerous guidelines providing assistance.

Are there additional issues when outsourcing?

- Generally when outsourcing is intended the data controller/data processor distinction must be scrutinised. A key question for consideration is: Will the Policy-maker maintain control or will a third party service provider assume control in relation to parts of the processing?
- Policy-makers should ascertain whether any transfers of data will be made outside of the EEA and also the technical and organisational security measures of the third party service providers.
- Where third party service providers are to be used, Policy-makers must also consider whether any contracts will be caught by the EU regulations governing public procurement.

DIRECT MARKETING

The principal EC Directive regulating direct marketing is Directive 2002/58/EC [9] (the 'E-Privacy Directive'). The instrument by which this Directive was transposed into the law of England and Wales was the Privacy and Electronic Communications (EC Directive) Regulations 2003

- The Directive seeks to govern the transmission of unsolicited marketing messages received via electronic means particularly by telephone, fax, text, photo messaging and email.
- The Directive is wide enough to include material promoting a charity or a political party's organisational aims. However it is considered that where

contact is made without a direct marketing aim that such communications would not be caught.

- Unsolicited marketing messages may not be transmitted via electronic means without the prior consent of the SNS user.

USER EXPECTATION OF PRIVACY

Many of the legal and ethical concerns surrounding privacy issues turn on a user's expectation of privacy.

- Article 8 – Right to respect for a person's private and family life. A SNS user's expectation of privacy must be considered.
- Article 11 – Right to freedom of peaceful assembly and association. A recent case of the European Court of Human Rights [10] held that storage of personal data relating to data subjects' political opinions affiliation and activities in violation of Article 8 will by that very fact constitute an interference with an individual's rights under Article 11.

CONFIDENTIALITY, INTERCEPTION AND SURVEILLANCE

The E-Privacy Directive places obligations on Member States to implement measures protecting the confidentiality of electronic communications. Member States are required to implement legislation prohibiting the unlawful interception and surveillance of communications, unless consent has been obtained. For example, the interception, monitoring and surveillance of communications is dealt with under the law of England & Wales by the Regulation of Investigatory Powers Act 2000 (RIPA).

INTELLECTUAL PROPERTY RIGHTS

The intellectual property rights of most relevance to the WeGov project are likely to be copyright and the database right. There are numerous EC directives dealing with certain aspects of copyright. In England and Wales the right is protected by the Copyright Designs and Patents Act 1988 (CDPA). Policy-makers should consider the following points:

Copyright

- Copyright arises automatically without the need for registration. The works may be primary i.e. literary, dramatic musical or artistic works or secondary/derivative works such as sound recordings, films, broadcasts and typographical arrangements. Primary works must satisfy the test of originality.
- The test of originality is applied differently between civil law countries (such as France, Germany, Italy) and common law countries (such as the UK). The UK's test is that of "skill labour and judgment". The civil law countries impose a higher test of the author's intellectual creativity. Nevertheless some EC directives have particularly stipulated that the higher test should be applied to certain categories of works. An example of this is the Database Directive.
- Assuming that copyright does subsist in an example of user generated content, legislation sets out some defences such as transient and temporary copying as well as 'fair use for the purposes of criticism, review and news reporting. The latter defence was relied upon by Google when sued by Copiepresse.

- Applying defences are not without their difficulties and consideration of the SNS's terms of use/service is necessary.
- The terms of use of SNS generally provide that the user grants the SNS with a non-exclusive royalty free license to use, copy, reproduce, process, adapt, modify, publish etc the user's content. Whether third parties are granted a right to use this content depends on the SNS concerned.

Database Right

In addition to the protection afforded to original databases under the UK CDPA 1988, the EC Directive, Directive 96/9/EC [11] (the 'Database Directive') distinguished between original databases and non-original databases. Original databases if satisfying the higher test of 'author's intellectual creation' are protected as copyright works, but non-original databases may also be protected by the standalone (sui generis) database right. In England and Wales non-original databases are protected under the Copyright and Rights in Database Regulations 1997 (SI 1997/3032).

- In addition to copyright protection websites may also claim protection under the database right.
- Provided SNS are able to satisfy qualification, it is arguable that the systematic and repeated extraction of comments from SNS may result in a reconstitution of a substantial part of the contents of the database, thus infringing this right.
- Cooperation with the SNS, extracting data with their consent is a solution, furthermore most SNS stipulate within their terms of use/service that they will only permit crawling done in accordance with their procedures and terms of use or with their explicit consent.

DEFAMATION

There is no specific EC Directive harmonising the law in this area, so we focus on the law of England and Wales. Here both the common law position and the Defamation Act 1996 must be considered.

Some key points for consideration:

- Authors, publishers and editors may be held liable for defamatory material.
- Unless the libellous material originates from the Policy-maker, it is unlikely that Policy-makers would be considered authors.
- A distinction is drawn between primary publishers (i.e. someone that authorises the defamatory material) and secondary publishers. Publishers that fall under the latter category may rely upon the statutory defence (s.1 of the Defamation Act). However once a secondary publisher is put on notice that the material is defamatory, they are unable to rely upon the statutory defence.

OBJECTIONAL POSTS

Policy-makers may from time to time come across offensive or objectionable posts submitted by SNS users. For example comments inciting race hate or posts victimising a user or group.

- Where these comments are published on a SNS the main concern Policy-makers would be faced with is whether or not to report comments to the SNS, bearing in mind Article 10 of the Human Rights Convention.

- On certain SNS, such as Facebook, where Policy-makers are able to create official pages, they do have the ability to remove such posts; but again any decision to remove material/content (via moderation) should bear in mind individuals' rights to freedom of expression.

IMPLICATIONS FOR WEGOV

In the area of privacy, there are significant implications for WeGov, and others looking to engage with SNS users in similar ways. Given the broad definition of personal data coupled with the potential reputation damage of policy-makers of not being 'squeaky clean', a safe position to take is that the information that needs to be collected and processed in WeGov should be considered personal data in almost all circumstances. Given the political nature of the data collected, it is likely that much of the data collected by Policy-makers through the use of the WeGov toolkit will also be sensitive data. Rather than adopting two procedures (i.e. one for personal data and one for sensitive data) it is considered that Policy-makers might wish to treat all data collected as sensitive. Furthermore, attempts to anonymise the data are unlikely to be effective. Therefore, data protection requirements will apply.

When the policy-maker uses the WeGov toolkit directly (e.g. installed as a product on a computer within their organisation, hosted on a remote machine under their control e.g. in a collocation data centre, or even installed at a cloud infrastructure provider such as Amazon EC2), then the policy-maker will be considered a data controller and hence they have corresponding obligations, e.g. to follow the 8 principles of the Data Protection Act in England and Wales. This limits how they can legitimately collect and process data.

Most significantly, unless there is *not* an expectation of privacy on the part of the SNS user (e.g. twitter user or posts to a public Facebook group) then there is a need to seek explicit informed consent in order to collect and process the users' data, e.g. any comments and posts they make or any details they expose on a profile page. The need to get consent in advance of processing data may well put off citizens when engaging with policy-makers, but on the other hand it provides a point at which the citizen can be fully informed on exactly what data is being collected, why, for how long, and how they can make access requests to this data. This aides transparency and openness, and hence has the potential to engender a higher degree of trust even if the level of participation is somewhat lowered. It will be interesting to see how this works in practice during the WeGov trials later in the project.

Even if there is not an expectation of privacy by the SNS user, e.g. for Twitter, data protection legislation still applies and there may still be a requirement to issue a fair processing information notice – provided that there is not disproportionate effort involved. This is a matter of judgement for the policy-maker on the cost-benefit of doing this and is likely this decision will have to be made on a case-by-case basis.

Under the provisions of RIPA it is considered that the WeGov toolkit would not be intercepting data during transmission. Any surveillance or monitoring of communications which is covert in nature would breach Article 8 of the Human Rights Convention. Whether surveillance or monitoring is covert raises the same debate of whether the information is within the public domain. Obtaining explicit consent would again resolve these uncertainties.

It is likely that some user generated content will satisfy the test of originality and that copyright will subsist: however it is considered that making this assessment for each example of user generated content would be problematic and unrealistic for policy-makers, and, as a result, it is recommended that policy-

makers take the defensive position of assuming that copyright subsists in all user generated content and again addresses this through explicit agreements with the user.

The use of SNS is bound by terms and conditions of use, typically embodied in an End User License Agreement (EULA) and often extended where access is automatic and through a software API. These terms and conditions may impose further restrictions on the collection and processing of data from SNS sites and in all cases need careful review in the context of what the policy-maker is seeking to achieve. SNS operators typically issue a privacy policy that states what they will do with data they hold for their users. This tends not to extend to allowing arbitrary third-parties, e.g. policy-makers, to collect and process the data. Therefore, unless there is clearly no expectation of privacy on the part of the user, then explicit consent is required from users when collecting their data, including provision of a privacy policy by the policy-maker.

The requirements of data protection, direct marketing legislation, monitoring of communication, SNS EULAs, and intellectual property law all point to the need for seeking explicit consent when collecting and processing data from SNS. This can be used as a 'catch-all' opportunity to cover the full range of issues, e.g. fair processing notices, privacy policies, informed consent etc.

When it comes to the policy-maker posting feedback or injecting comments on SNS, in such circumstances the Policy-maker would be considered a publisher as they are likely to control what material ought to be fed back into the SNS. Depending on the level of control given to Policy-makers it might be sufficient to constitute editorial control. Where the Policy-maker is put on notice that the material to be published contains libellous materials, the section 1 defence fails. However, a Policy-maker might be able to avail itself of other defences such as justification/truth or fair comment in the public interest. When creating links within a SNS for the purposes of initiating or adding to debate, caution is recommended. Where the link transfers the SNS user to libellous material, Policy-makers again might be considered publishers and/or editors. When injecting content into SNS, policy-makers should make an assessment on material that is potentially libellous. This will necessitate a balancing act between information which ought to be brought to the public's attention and the potential risk to the policy-makers. Furthermore any assessment should bear in mind Article 10 of the Human Rights Convention (Freedom of Expression).

Finally, in order to lower the barrier to take-up of the WeGov technology, the WeGov project has discussed the possibility of cloud computing as a way to run the toolkit without the need for a policy-maker or their organisation to install and maintain local computing infrastructure. This could be particularly attractive to smaller organisations, e.g. a local council. Here it is likely that the cloud provider used to host the software would be considered as a data processor and not a data controller. Therefore, it is still the responsibility of the policy-maker to ensure that the cloud provider has suitable measures in place to meet the requirements of data protection (which includes geographical constraint over the location of data as well as security of the data) and that these are included in the contract with the provider. Many cloud providers disclaim responsibility and make it clear that this is up to the customer to meet these requirements [12], although there are some exceptions [13]. Therefore, if a third-part is involved in hosting tools used to process personal data from SNS, then in addition to the general points above, specific issues such as the location of the data and sub contracting arrangements need to be addressed.

The issues above are reflected in the three WeGov scenarios where any attempt to solicit opinion, e.g. through creating a Facebook group or conducting a survey, will be done using explicit consent, and any attempt to collect and process already existing information will be limited to information where there is not an

expectation on the part of the SNS user of privacy and hence consent can be considered as implicit.

INFORMATION SECURITY RISK ASSESSMENT

Extending the specific legal and ethical analysis above, WeGov has initiated an information security risk assessment process to identify a wider set of security requirements that need addressing for the WeGov toolkit to both help the policy-maker comply with legal requirements and to ensure that the results of using the toolkit have required levels of authenticity, integrity, traceability and security. In WeGov, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) [14] has been applied. OCTAVE is a strategic assessment and planning technique for security proposed by CERT (Computer Emergency Response Team) Coordination Centre. It is self-directed, that is, a small team of people from the operational (or business) units and the IT department work together to address the security needs of the organisation. In this way, WeGov applied CERT based on the knowledge of the project partners of the current state of security, identify risks to critical assets, and set a security strategy. The process identifies information-related assets (e.g., information and systems) that are important to the organisation; focuses risk analysis activities on those assets judged to be most critical to the organisation; considers the relationships among critical assets, the threats to those assets, and vulnerabilities to those threats (both organisational and technological) in an operational context - how they are used to conduct an organisation's business and how those assets are at risk due to the security threats; and creates a practice-based protection strategy for organisational improvement as well as risk mitigation plans to reduce the risk to the organisation's critical assets. The analysis has to be done in each specific context and from each stakeholder perspective, so for example in the Hansard Society scenario information assets include: decision maker topic seeds;citizens comments on topics; citizens' personal and sensitive data; results of data processing results; decision maker profile information; decision maker credentials; decision maker messages/comments; and SNS group participants. These are then assessed against threats to integrity, authenticity, confidentiality, availability or other ways in which they could be compromised. Having assessed the assets and threats, a set of mitigation approaches were used to derive a general set of WeGov security requirements. The following table lists these requirements. Note that we focus here on the technical measures that WeGov may address. Other mitigation approaches are of procedural or organisational nature and cannot be addressed by WeGov software (e.g. staff training, installation of anti-virus, intrusion detection mechanisms…).

Requirement ID	Requirement
Sec-1	Enable the usage of integrity mechanisms (e.g. hash algorithms, digital signature) for data while in transit to prevent unauthorised modification.
Sec-2	Allow user identification and authentication when interacting with WeGov tools/components.
Sec-3	Specify a procedure to allow citizens to access/correct/amend their personal information once stored in WeGov.
Sec-4	Allow the logging of actions done on data (who did what and when) in order to create an audit trail.
Sec-5	Allow the specification of fine granularity security policies to regulate access to data or services within WeGov.

Sec-6	Fine granularity security management policies allowing policy-makers to delegate some privileges to their staff.
Sec-7	Use available authorisation systems on SNS to specify policies for preventing unauthorised modification of data.
Sec-8	Specify a coherent security policy over data whether it is on the policy-maker website or the SNS sites.
Sec-9	Use confidentiality mechanisms (e.g. encryption) for content while in transit to prevent unauthorised access.
Sec-10	Indicate where possible whether the SNS terms and conditions do not allow accessing the data (which may include personal and sensitive information).
Sec-11	Use secure algorithms and protocols for transporting credentials on the wire.
Sec-12	Data backup to assist the disaster recovery process.
Sec-13	Logging of any detected security breaches, deliberate or accidental, and whether they were successful or not to allow security effectiveness to be measured.
Sec-14	Use the most recent and stable versions of libraries and software building blocks within WeGov.
Sec-15	Delete any confidential information as soon as it is not needed.
Sec-16	Support high availability of data and processing.
Sec-17	Use mechanisms to prevent unfair usage of the system e.g. limited number of posts and words count per day.
Sec-18	Allow resetting of policy-maker credentials.
Sec-19	Allow notification of users if serious security breaches have been detected that would cause damage to their data.
Sec-20	Allow the exclusion of users from the WeGov platform if they do not abide by the usage policy.
Sec-21	Collect the minimum amount of personal data that will permit the previously-stated purposes of processing.
Sec-22	Use an inter-organisational security model to support secure interactions between the policy-maker and a potential WeGov provider.
Sec-23	Support multiple policy-makers simultaneously.
Sec-24	Support collection of user (citizen) consent for data usage for specified purposes.

CONCLUSIONS

In this paper we have examined several scenarios involving policy-makers or similar stakeholders interacting with citizens through the use of open public social networking sites. The processes involved include ones where the policy-maker is interested in existing discussions and debate and using these to gauge public opinion or to discover what is currently a hot topic and hence needs attention, but also processes where the policy-maker wants to instigate a discussion and

stimulate comment in a more structured way, e.g. using an online survey or a Facebook group. These modes of interaction have legal, ethical and information security implications, in particular privacy and data protection, which both limit the specific implementation approach, but also provide an opportunity for high levels of transparency and trust between policy-maker and citizen through the need for clear statements of what data will be collected and why followed by explicit consent. There are many technical challenges that now need to be overcome to deliver the software tools that will enable these new ways of working for policy-makers and this is now the subject of the next phase of the project.

ACKNOWLEDGEMENTS

The WeGov project (no. 248512) is funded with support from the European Commission under the SEVENTH FRAMEWORK PROGRAMME THEME ICT 2009.7.3 ICT for Governance and Policy Modelling.

REFERENCES

[1] http://www.give-your-voice.eu/
[2] http://digitaldialogues.org.uk/reports/digital-dialogues-phase-three/
[3] http://en.wikipedia.org/wiki/Gorleben
[4] http://www.spiegel.de/international/germany/0,1518,672147,00.html
[5] http://www.gesis.org/beta/prototypen/irm/
[6] Privacy and Human Rights: An International Survey of Privacy Laws and Development; published by Electronic Public Information Center and Privacy International; 2000.
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.
[8] Opinion 1/2010 on the concepts of “controller” and “processor” adopted by the Article 29 Working Party on 16 February 2010; 00264/10/EN (WP 169).
[9] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
[10] Segerstedt-Wiberg and ors v Sweden App. No. 62332/00. 6 June 2006
[11] Directive 96/9 EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases.
[12] E.g. see Customer Terms for Amazon Web Services http://aws.amazon.com/agreement/
[13] http://www.euroinvestor.co.uk/news/story.aspx?id=11155721
[14] http://www.cert.org/octave/